Decoding Data Privacy

Vendor Contracting at the Intersection of Employment & Commercial Litigation

August 2026

Seyfarth Shaw LLP

Legal Disclaimer

This presentation has been prepared by Seyfarth Shaw LLP for informational purposes only. The material discussed during this webinar should not be construed as legal advice or a legal opinion on any specific facts or circumstances. The content is intended for general information purposes only, and you are urged to consult a lawyer concerning your own situation and any specific legal questions you may have.

Speakers

Kristine Argentine
Partner
Chicago Office
kargentine@seyfarth.com

Ada Dolph
Partner
Chicago Office
adolph@seyfarth.com

Paul Yovanic
Partner
Chicago Office
pyovanic@seyfarth.com

Ala Salameh
Associate
Chicago Office
asalameh@seyfarth.com

Agenda

1 | Telephone Consumer Protections Act (“TCPA”)

2 | California Invasion of Privacy Act (“CIPA”)

3 | Cybersecurity and Data Breach

4 | Illinois Biometric Information Privacy Act (“BIPA”)

5 | Illinois Genetic Information Privacy Act (“GIPA”)

6 | Key Takeaways for U.S. Vendor Contracting

7 | Cross-Border Considerations

TCPA

Telephone Consumer Protection Act (TCPA)

Overview

The Basic Restrictions and Requirements

- No calls or texts to a **cellular phone** using any **automatic telephone dialing system** or an **artificial** or **prerecorded voice** the call is made:
  - For “emergency purposes”
  - With the prior express consent of the called party
- No calls to a **residential telephone line** using an **artificial or prerecorded voice** without prior express consent unless an emergency purpose or is otherwise exempted.
- No **telephone solicitations** to individuals on the **DNC** unless there is an established business relationship or prior permission
- Honor **reasonable request to opt out** within 10 business days
- No telephone solicitations before 8 am or after 9 pm

Telephone Consumer Protection Act (TCPA)

Litigation Trends

TCPA Trends

- No longer seeing a lot of claims based on use of an auto-dialer
- Trend in “after hour” marketing cases has slowed
- Rise in pre-recorded voice cases based on new AI technologies
- Increase in DNC cases where there is a lack of consent due to numbers being re-assigned
- Rise in demands and litigation related to failures to honor opt out requests
  – Especially in the text messaging context

Telephone Consumer Protection Act (TCPA)

Vendor Considerations

Vendor Considerations

- Understand the technology being utilized and whether it could qualify as an auto-dialer under TCPA
- Communicate with vendor about who is collecting consent and how that information is maintained
- Understand the different TCPA requirements depending on the technology being utilized (pre-recorded calls, texts, etc.)
- Know what mitigation efforts the vendor is covering and what will need to be covered internally
  - Reassigned number review
  - National Do Not Call Registry
  - Internal do not call list
  - After-hour calls/texts
- For consent-based SMS databases, know how incoming messages are analyzed and treated for opt out purposes
- Do not rely solely on the vendor for policies and training – have internal procedures as well.
- Make sure the vendor is aware of the states in which it is contacting individuals
- Insurance and indemnity

CIPA

Website Tracking Technology Litigation - Overview

State and Federal wiretap and other data privacy-based statutes

Federal Wiretap Act

California Invasion of Privacy Act, it is illegal to intentionally record or eavesdrop on telephone calls without the consent of all parties.

- **California Penal Code 631** – third party wire-tapping and in-transit interception of content
- **California Penal Code 632** – monitoring or recording confidential communications
- **California Penal Code 638.51** – Trap and trace – routing/addressing information
- **California Penal Code 637.2** - $5,000 statutory damages per violation

Other two-party consent states statutes or statutes requiring consent for transfer or sharing of data (VPPA, GIPA)

Website Tracking Technology Litigation – *Litigation Trends*

- Targeting websites utilizing any tracking technology, analytics tools, data aggregation tools, AI tools where the data is sent to a third party and where there is no cookie management system on the website to make disclosures or capture consent

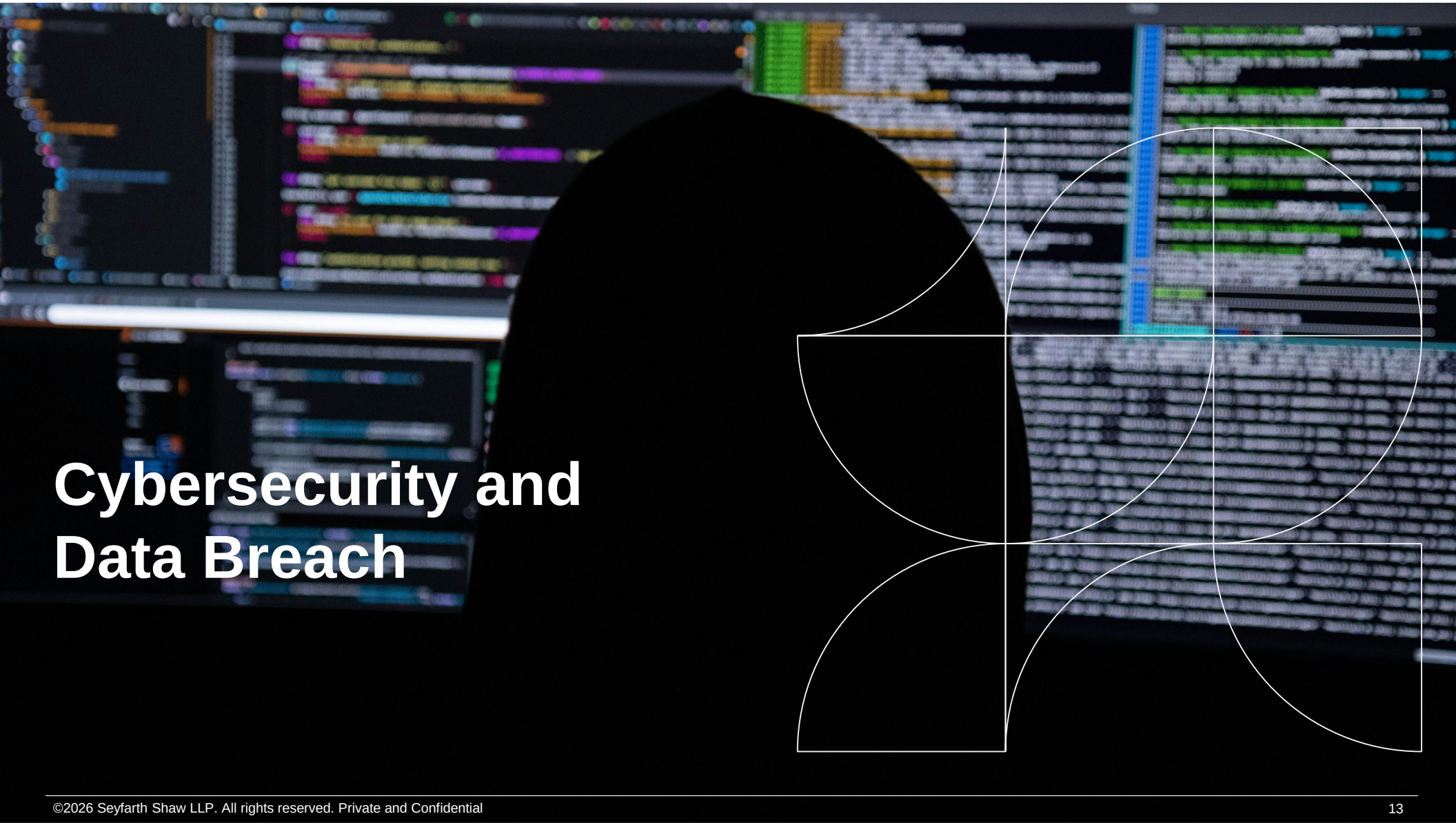
- Targeting websites utilizing tracking technology through pixels or cookies where the cookie management system is not operating consistent with the user's selections

- Looking for technology that is operated by big tech and marketing companies where the data could be used through their own algorithms for other purposes

- Looking for technology to be embedded in particularly sensitive or substantive parts of websites (password protected portals, search bars, check-out processes)

Website Tracking Technology Litigation – *Vendor Considerations*

- There could be lots of different vendors at play here:
  - Website operators
  - Digital marketing partners
  - IT partners or service partners controlling certain functionalities of the website (checkout, chatbots, search functions)
  - Cookie management vendors
- Legal considerations and risk in terms of:
  - What technology is being implemented and how it is configured
  - What data is being sent through the technology
  - What the vendors/partners are permitted to do with the data
  - What security measures could be implemented to restrict certain types of data or anonymize the data
  - Indemnification and insurance



Cybersecurity and Data Breach

Cyber Security

Vendor Considerations

Vendor Considerations

- **Scope of data and processing.** Identify the categories of data the vendor may process

- **No secondary use.** Prohibit/limit other uses of customer/ employee data outside the contracted services without approval.

- **Security controls appropriate to the vendor.** Require Multi-factor authentication (MFA), encryption, least privilege, named-user accounts, logging, access reviews, vulnerability management, data segregation, secure deletion, and reasonable assurance such as SOC 2, ISO 27001, or equivalent evidence where appropriate.

  – **Subcontractor controls**

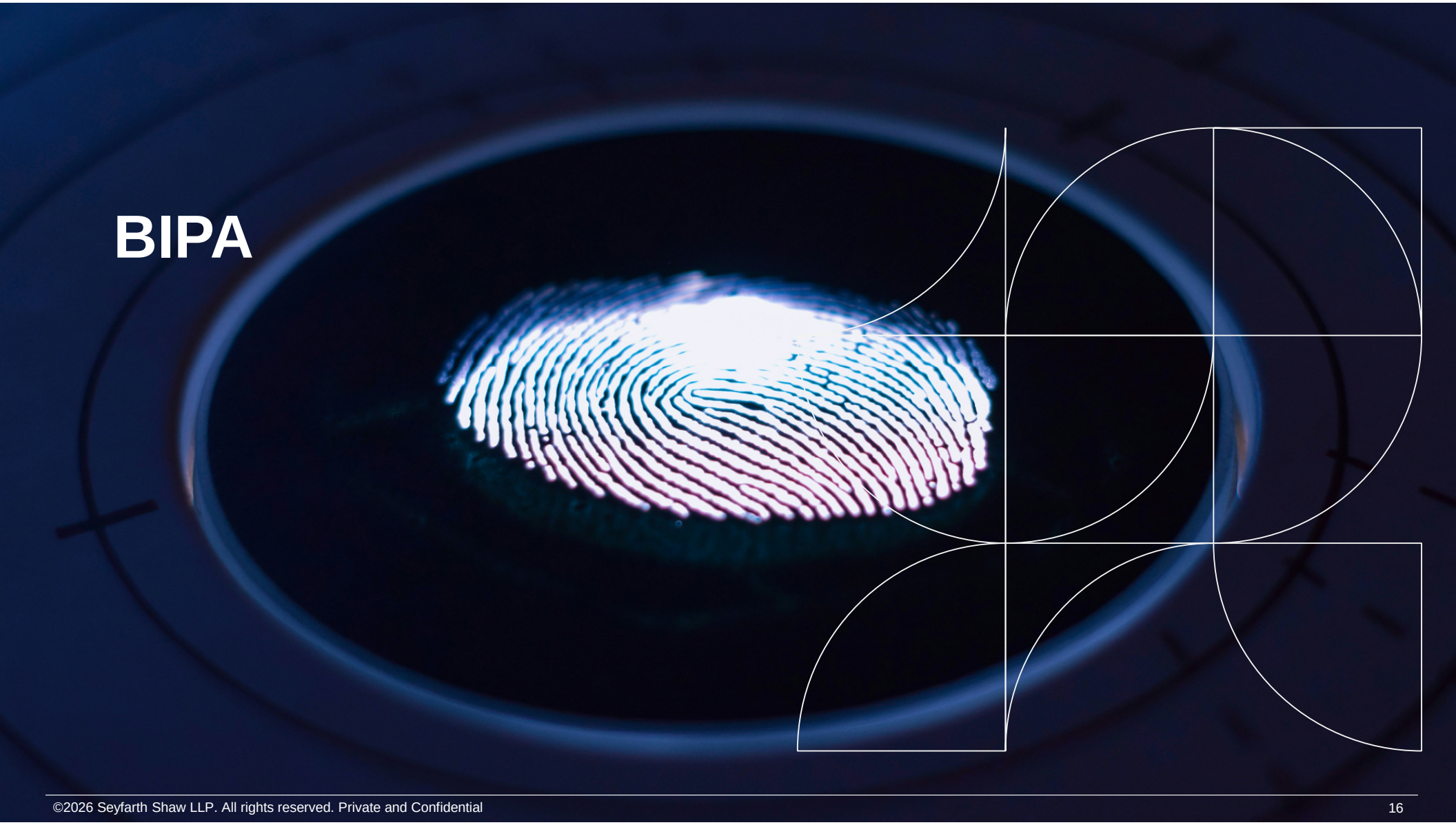
Cyber Security

Vendor Considerations

Vendor Considerations

- **Incident notice and cooperation.** Require prompt (24/48/72 hr) notice of actual or suspected unauthorized access, disclosure, loss, or other data incident and include:
  - **Operational escalation**
  - **Control over legal determinations and notices**
  - **Forensic preservation and cooperation**
- **Risk allocation.** Include vendor responsibility for reasonable breach-response costs caused by its failure, and carveouts or higher caps for higher risk incidents
- **Liability, indemnity, and insurance**

BIPA



Illinois Biometric Information Privacy Act (BIPA) Overview

- Enacted in 2008
- Only standalone biometric privacy law in U.S. with private right of action, liquidated damages, and attorneys' fees.
- More than 2,000 lawsuits filed since enactment – majority in and after 2019
  - (following *Rosenbach* standing decision).
- Well over $1B in BIPA settlements and one verdict.
- "Biometric Information" means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual.
- "Biometric Identifier" means a retina or iris scan, fingerprint, voiceprint, or scan of hand of face geometry.
- Liquidated damages of $1,000 for each negligent violation or $5,000 for each reckless violation. ("may" recover)

BIPA Requirements

- **14/15(a) –** develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric information **or** identifiers.
- **14/15(b) –** provide written notice and obtain written consent before capturing, collecting, purchasing, receiving through trade, or otherwise obtaining a person's biometric information **or** identifiers.
- **14/15(c) –** prohibit the sale, lease, trade or profit of a person's biometric information.
- **14/15(d) –** prohibit the disclosure of biometric information or identifiers without consent or as required under the Act.
- **14/15(e) –** store, transmit, and protect from disclosure all biometric identifiers and biometric information using the reasonable standard of care within the private entity's industry and in a manner that is the same as or more protective than the manner in which other confidential and sensitive information is stored, transmitted, and protected.

BIPA Litigation Trends

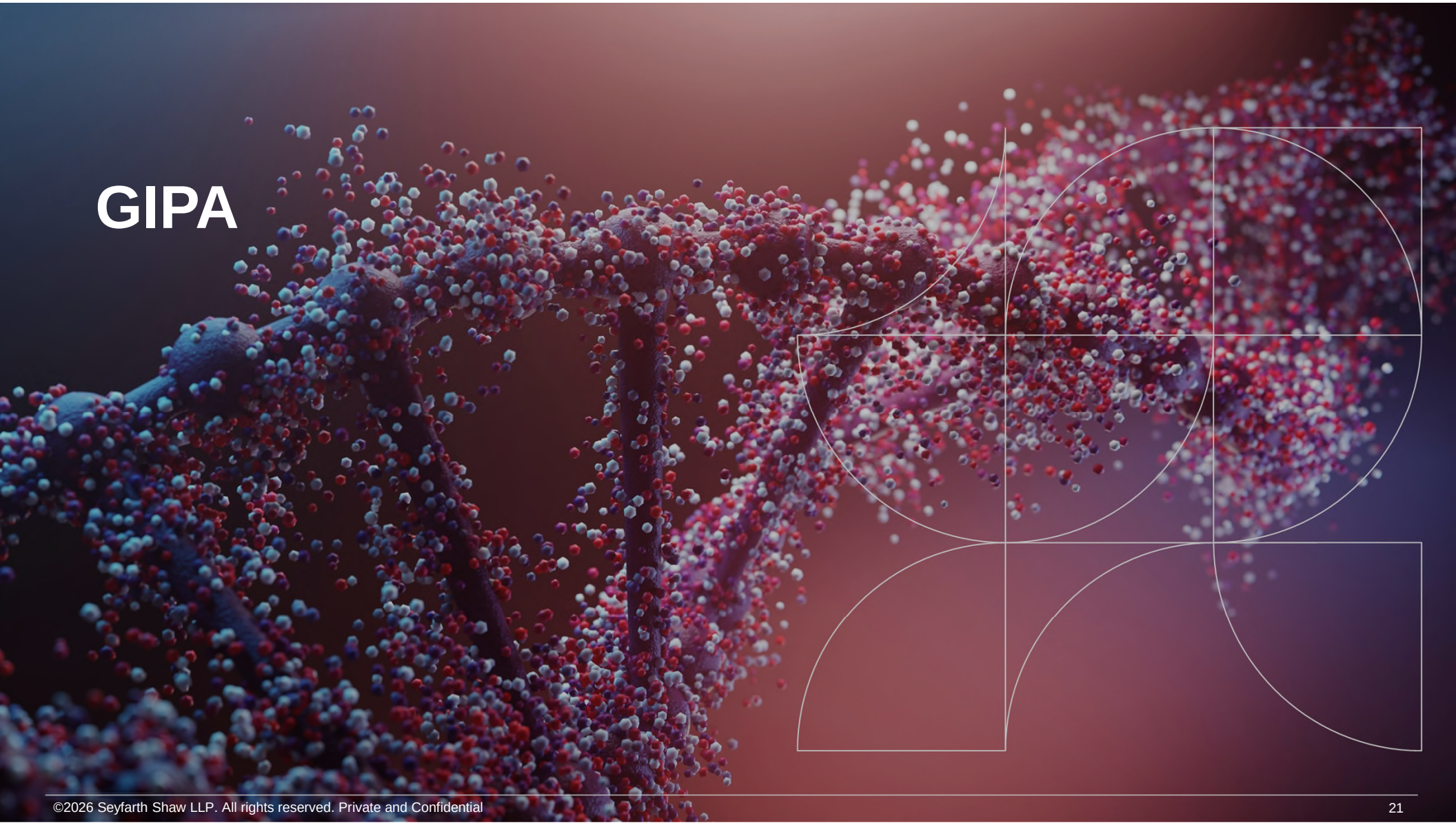
- Hourly employees in all industries using finger scan time clocks (restaurants, hotels, etc.)
- Supply chain logistics companies using driver facing cameras
- Retailers offering online virtual try-on features
- Medical providers using finger scan medicine cabinets
- Security identification screenings
- Facial recognition in retail stores (Clearview)
- Automotive industry (voice command & driving assistance)

Illinois Biometric Information Privacy Act (BIPA)

Vendor Considerations

- Define the technology and data flow.
- Allocate notice and consent responsibilities.
- Restrict use and disclosure.
- Establish retention and deletion requirements.
- Require appropriate security and incident response.
- Address audit rights and risk allocation.

GIPA



Illinois Genetic Information Privacy Act (GIPA) - Overview

- Employer-specific provisions (limited, imprecise)

(410 ILCS 513/25)
Sec. 25. Use of genetic testing information by employers

(c) An employer, employment agency, labor organization, and licensing agency shall not directly or indirectly do any of the following:

(1) solicit, request, require or purchase genetic testing or genetic information of a person or a family member of the person, or administer a genetic test to a person or a family member of the person as a condition of employment, preemployment application, labor organization membership, or licensure

Illinois Genetic Information Privacy Act (GIPA) - Overview

Two decades of mostly *silence . . .* until 2017

- GIPA is very similar to BIPA--mimics language, structure, and damages provisions.
- Focus of the statute is on the use of genetic testing to determine suitability for insurance coverage or employment.
- Like BIPA, it too, contains no statute of limitations, and no definition of what constitutes a violation of the statute.
- **Notably, consent is NOT a defense**. Under the strict wording of the statute, arguably the collection of the genetic information constitutes the statutory violation.
- GIPA provides minimum statutory damages of $2,500 per negligent violation and maximum statutory damages of $15,000 per intentional violation or actual damages, whichever is greater.
- Federal counterpart, *Genetic Information Nondiscrimination Act* (GINA) passed in 2008
  - "Genetic information"
    - "Family medical history"
  - "Condition of employment"

Illinois Genetic Information Privacy Act (GIPA)

Litigation Trends

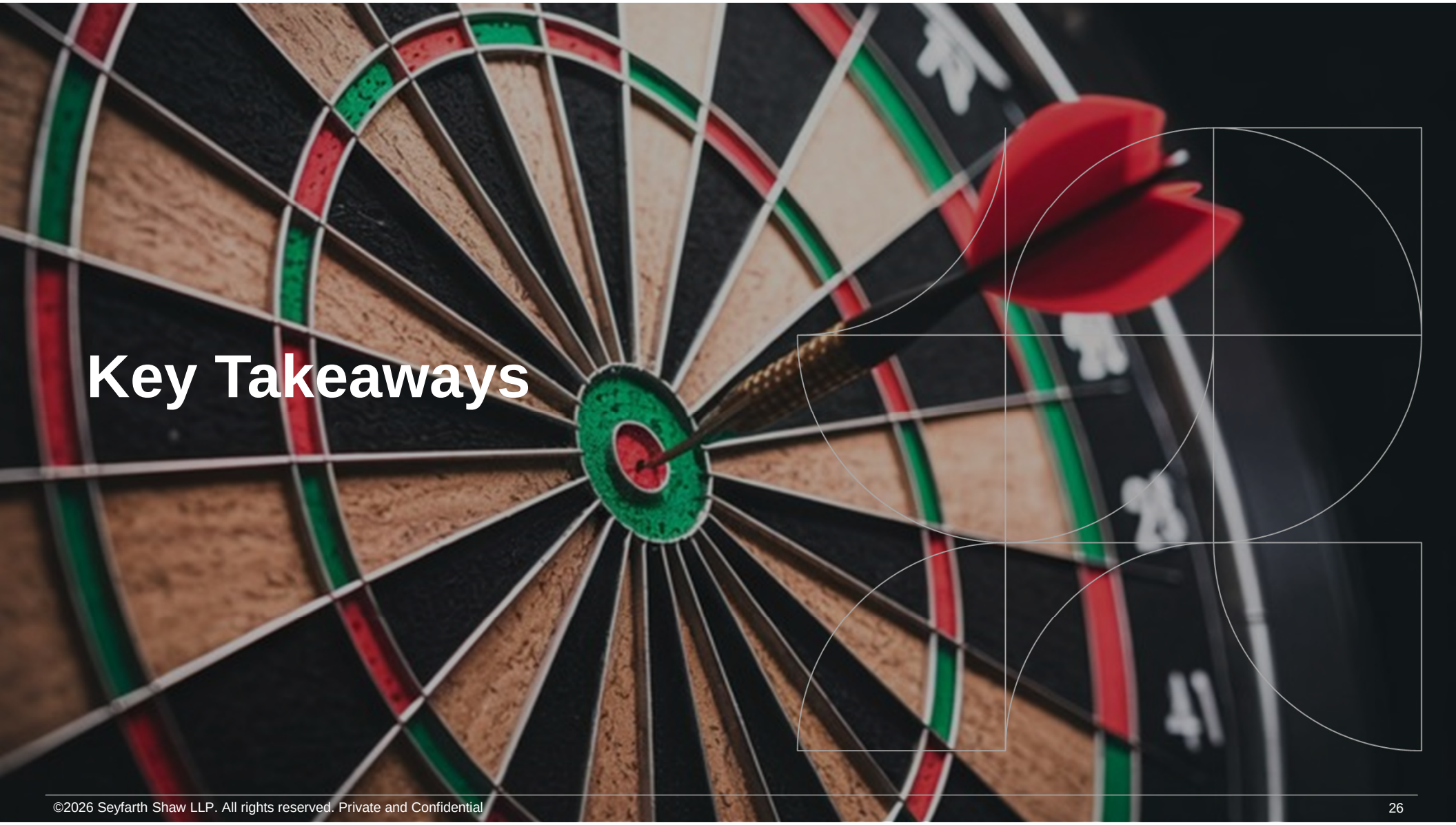
- Challenged employment practices
  - Pre-employment medical questionnaires
  - Post-offer medical screenings
  - Occupational health and wellness programs
  - Ongoing medical surveillance
- Targeted industries
  - Transportation and logistics
  - Common carriers
  - Healthcare, pharmaceutical companies
  - Manufacturing employers
- Role of employers *versus* vendors

Vendor Considerations

- Vendors and agreements to consider
  - Occupational health
  - Medical examination providers
  - Wellness program provider
  - Targeted screening services

- Employer Protections
  - Legal compliance
  - Limited data transmission to employer
  - Limited employer access to data
  - Indemnification
  - Require arbitration provision in vendor agreements
  - Control of tools, protocols, staffing

Illinois Genetic Information Privacy Act (GIPA)



Key Takeaways

Key Takeaways for U.S. Vendor Contracting

- Indemnification
- Insurance
- Choice of law and venue
- Arbitration
- Party responsible for legal compliance (and placement of clause within agreement)
- Limits on liability- efforts of third-party providers to absolve themselves of obligations
- Agency theory – alignment of practice and language regarding control of technology and practices
- Data breaches – storing data in different places to reduce risk

Cross-Border Considerations

Cross-Border Considerations

- Understand where the data goes.
- Identify transfer and localization requirements.
- Evaluate the destination country and access risks.
- Control sub-processors and onward transfer.
- Coordinate operational responsibilities.
- Address restricted countries and contractual risks.

SCAN ME

CLE: NEW PROCESS

Please scan the QR code and complete the digital attendance verification form to receive CLE credit for this program.

You will need:

1. **Title:** Vendor Contracting at the Intersection of Employment, Privacy, and Commercial Litigation
2. **Date Viewed:** _August 6, 2026_____
3. **Attendance Verification Code:** SS____

State-specific CLE credit information can be found in the form.

Questions?

thank you!

For more information, please contact:

Kristine Argentine
email: kargentine@seyfarth.com

Ada Dolph
email: adolph@seyfarth.com

Paul Yovanic
email: pyovanic@seyfarth.com

Ala Salameh
email: asalameh@seyfarth.com